Journal of Advanced Research in Cloud Computing, Virtualization and Web Applications
Volume 1, Issue 2 - 2018, Pg. No. 15-18
Peer Reviewed Journal
Research Article

Security Protocols for Internet of Things (IoT)-A Survey

Sandeep Kaur[1], Shifali Katoch[2]

[1]Assistant Professor, Dept. of Computer Science, St. Soldier College Hadiabad, Phagwara.
[2]Assistant Professor, Dept. of Computer Science, DAV University, Jalandhar.

Abstract

In the next upcoming scenario, Internet of Things (IoT) is expected to have a great rise in coming future years with a mixture blend of various technologies together such as nanotechnology, cognitive computing, wireless technology, big data and cloud computing. With this blend of combination, the wide use of IoT leading to Internet of Nano Things (IoNT) will leave last longing impressions in the life of human beings and change the science technology completely. This paper presents an approach to study various IoT security protocols that are currently available for use.

Keywords: IoT, IoT Security, Security Protocols

Introduction

With emergence of internet in daily life and exchange of information among different objects, a new phase of information interchange rise known as Internet of Things. Some of the important definitions of IoT are discussed below. According to RFID group, IoT is "The worldwide network of interconnected objects uniquely addressable based on standard communication protocols". ITU defines IoT as "from anytime, anyplace connectivity for anyone, we will now have connectivity for anything.[1] Internet of Things (IoT), a thoroughly characterized interconnection of network, is internet based architecture of information interchange of global goods and services.[4] IoT, a widely used concept but not completely clear expression, brought a new sense of innovation and positivity to make smart objects work together. Devices meant for daily use, either in household or in globally recognized organizations is connected via internet.[3]

Security is one of the fundamental factors in IoT to protect the communication among devices and objects. But with the increase in the applications, its security risk also increases rapidly. Traditional methods for security are no longer suited as objects are exposed to variety of risks.[4] This is mainly due to IoT's integration with the internet. Current trends in IoT include concepts such as Machine-to-Machine (M2M) communications, Low Power Wireless Personal Area Networks (LoWPAN), Wireless Sensor Networks (WSN) and technologies such as Radio-Frequency Identification (RFID). Electrical and Electronics Engineers (IEEE) and the Internet Engineering Task Force (IETF) are the standardized organizations that reflects the effect caused by these current trends towards the security technologies as well as security risks and also on the communication design for IoT. Security Technologies form a protected wireless stack of different protocols for communication to reach a certain criteria of reliability, proper connectivity to internet as well as to power.[5]

Throughout this survey, we mainly focus on different standardized protocols currently available for security purpose.

Security Challenges

IoT faces a number of security challenges that are mainly based on internet. These challenges expose the objects and devices to high risks that may raise the questions regarding security in IoT. One of the challenges of security is authentication, which is the process of checking the

Corresponding Author: Sandeep Kaur, ssistant Professor, Dept. of Computer Science, St. Soldier College Hadiabad, Phagwara.
E-mail Id: sndpbhllr@gmail.com
Orcid Id: https://orcid.org/0000-0001-7835-3170
How to cite this article: Kaur S, Katoch S. Security Protocols for Internet of Things (IoT)-A Survey. *J Adv Res Cloud Comp Virtu Web Appl* 2018; 1(2): 15-18.

validation of the user in communication. But most of the devices and objects are constrained to use authentication due to the lack in term of resources and thus expose the user to risk.[5] Another challenge faced by IoT is data integrity. Data integrity implies the correctness of data and in term of IoT, it means data shared through sensors and resources remain untouched. Data in IoT may become vulnerable as some times it is not monitored completely on internet and left unprotected.[5] Privacy or trust is another issue in IoT. Trust is an abstract concept that can shield concrete structure, and can provide uniform decision-making for heterogeneous and multi-domain IoT.[4] But data could be breached intentionally or unintentionally and thus causes the loss of trust from users.

Above discussed are the most common challenges faced by IoT. In the next section we will discuss a servey regarding security protocols to overcome the security issue and present it as a trust-worthy asset.

Security Protocols

We research study by identifying the protocols designed to support Internet communications with sensors and devices in the IoT, which are the main focus of our study throughout the survey.[9] In this paper we have also discussed the security requirements that need to be met by these mechanisms to secure communications, using such protocols.

PHY and MAC layer Protocol

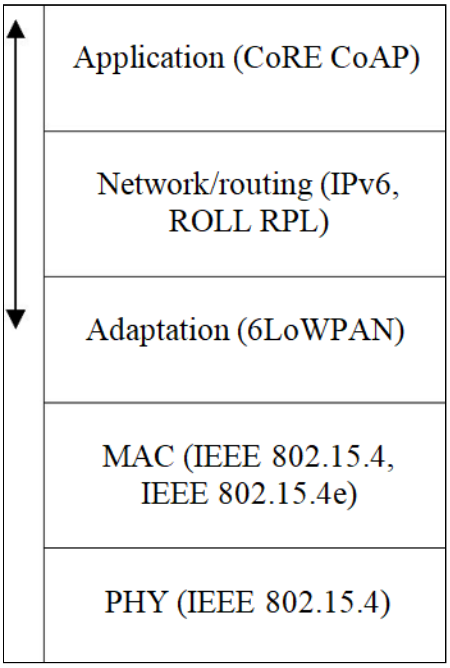
Application (CoRE CoAP)
Network/routing (IPv6, ROLL RPL)
Adaptation (6LoWPAN)
MAC (IEEE 802.15.4, IEEE 802.15.4e)
PHY (IEEE 802.15.4)

Figure 1.Communication Protocols in the IoT[9]

The communication protocols available or being designed at the IEEE and IETF currently enable a standardized protocol stack discussed in[1] and illustrated in Figure 1.

IEEE 802.15.4 and IEEE 802.15.4e are the commonly used standards in PHY and MAC. It is designed to support communication between nodes and a designed format for source and destination addresses. This protocol is meant for a good power efficiency which was earlier a drawback of traditional networks. IEEE 802.15.4 is best suitable to wireless communication environment with low energy requirement. IEEE 802.15.4 draw a base for standard technologies such as 6LoWPAN or CoAP at higher layers and adopted as industrial WSN standards. IEEE 802.15.4 act as a manager to the physical Radio Frequency (RF) transceiver of the sensing device, and also manages the channel selection and energy and signal management.[5] The IEEE 802.15.4 standard supports 16 channels in the 2.4 GHz Industrial, Scientific and Medical (ISM) radio band. One of the security factor i.e. Reliability is introduced at the PHY protocol by employing the Direct Sequence Ultra Wideband (UWB), Chirp Spread Spectrum (CSS), and Direct Sequence Spread Spectrum (DSSS) modulation techniques. As above discussed reliability is the main goal of these modulation technologies by changing and modifying the information being communicated over, so even if the power is low, it is possible to acquire more bandwidth with better Signal to Noise (SNR) ratio to get minimum interference along the frequency bands at the receiver end.[10] Since the data frames in PHY occupy less space, approximately 128 bytes, thus these packets minimizes the probability of error occurrence in wireless communication environment.[7]

The MAC layer manages data service as well as other operations such as accesses to the physical channel, guaranteed time slots, network beaconing, validation of frames, node association and security. The MAC standard is used to distinguish sensing devices by its capabilities and roles in the network. A Full-Function Device (FFD) is able to coordinate a network of devices; on the other hand other devices (of type RFD or FFD) are capable to communicate by using only Reduced-function device (RFD) [6]. IEEE 802.15.4 can support network topologies such as peer-to-peer, cluster and star networks by using RFD and FFD devices. IEEE 802.15.4 devices may be identified using either a 16-bit short identifier or a 64-bit IEEE EUI-64 [20] identifier.

Regarding the formatting of data to be transmitted, the IEEE 802.15.4 standard defines four types of frames to format data that need to be transmitted over a network: data frames, acknowledgment frames, beacon frames and MAC command frames. Collisions are managed in the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) Access method during data communications or, in alternative, establishment of a super frame in the perspective of which applications with predefined bandwidth requirements may store and use one or more special time slots is done by coordinator.[8] In this situation, signal frames or beacon frames act as the confines of the super frame and provide synchronization to other devices, as well as configuration information.

IEEE 802.15.4 has its own constraint as it is not well suited for application having some real time constraints. This constraint is removed by IEEE 802.15.4e which was earlier proposed in the form of the Time Synchronized Mesh Protocol (TMSP) where time synchronized frequency channels conflict with external interference and multipath fading. The infrastructure and design defined in IEEE 802.15.4e is an extension of IEEE 802.15.4 standard with some extra advantage in case of time constraint applications. In IEEE 802.15.4e devices and objects are synchronized to a structure of slot frame, a group of slots repeating its slots over time. For every active slot, a schedule directs the neighbor with whom a given device communicates with, and on which channel offset.[1]

Adaptation (6LoWPAN) Protocol

One core characteristic of the Internet architecture is that through it heterogeneous link-layer technologies enables packets to traverse interconnected networks, and the mechanisms and adaptations required to transport IP packets over particular link-layer technologies are defined in appropriate specifications. Same goal is considered in the IETF IPv6 over Low-power Wireless Personal Area Networks (6LoWPAN) working group was formed in 2007 to generate a specification which is capable of enabling the transportation of IPv6 packets over low-energy IEEE 802.15.4 and similar wireless communication environments. 6LoWPAN, a key technology to support Internet communications in the IoT, and one that has changed a earlier opinion of IPv6 as being impractical for constrained low-energy wireless communication environments.[7] The 6LoWPAN adaptation layer brought out a good example of how optimizations and cross-layer mechanisms may enable standardized communication protocols for the IoT, and make it capable to enables IPv6 end-to-end communications between restrained IoT sensing devices and other similar or more powerful Internet entities, thus providing the required support for the constructing of future IPv6-based distributed sensing applications on the IoT.[7] The 6LoWPAN adaptation layer plans the services required by the IP layer on the services provided by the IEEE 802.15.4 MAC layer. Currently no security mechanism is defined in 6LoWPAN but it provides a through guideline for routing mechanism.

Network/ Routing (IPv6, ROLL RPL) Protocol

The Routing Over Low-power and Lossy Networks (ROLL), a IETF working group formed with a strategy to achieve routing solution designs for IoT applications.[10] In 6LoWPAN environments, the current approach to routing is materialized in the Routing Protocol for Lossy Networks (RPL)[1] Protocol and Low power. RPL provides in reality a framework that is adaptable to the requirements of particular classes of applications rather than providing a generic approach to routing.[2] Instead of adopting routing strategies of 6LoWPAN with some challenging constraints over inherent specification of application and devices employment, RPL adapt the routing requirement by assuming its consequences. RPL provides cryptographic algorithms' employment and thus provides a sense of confidentiality. RPL offers support for protection, data authenticity, semantic security, against replay attacks, confidentiality and key management.[9] Levels of security in RPL include Unsecured, Preinstalled, and Authenticated. RPL attacks include Selective Forwarding, Sinkhole, Sybil, Hello, Black hole, Flooding, Wormhole and Denial of Service attacks.

Application (CoRE, CoAP) Protocol

A set of techniques are implemented by the CoAP[12] protocol to compress application-layer protocol metadata without affecting the application Inter-Operability, in conformance with the Representational State Transfer (REST) architecture of the web. Currently designed for only UDP communications over 6LoWPAN, CoAP can also meant to adopt transport-layer approaches with features more close to protocols such as the Transmission Control Protocol (TCP). Through Application-layer communications, IoT sensing applications may get enabled to interoperate with existing Internet applications without requiring any translation mechanisms or specialized application oriented code.[4] CoAP constraints the HTTP dialect to a subset that is well suitable to the 6LoWPAN's restricting sensing devices, and may enable abstracted communications between applications, users and such devices, in the perspective of IoT applications. A request and response communications model is provided by CoAP protocol between application endpoints and thus enables the usage of key concepts of the web, namely the usage of URI addresses to recognize the resources available on restricted sensing devices.[5] At the application-layer, the protocol may maintain end-to-end communications between restricted IoT sensing devices and other Internet entities, by using only CoAP or in substitute by translating HTTP to CoAP at a forward or reverse gateway. Messages in the CoAP protocol are interchanged asynchronously between two endpoints, and used to transport CoAP requests and responses. To secure CoAP messages, the CoAP Protocol defines bindings to DTLS (Datagram Transport-Layer Security), along with a few mandatory minimal configurations appropriate for restricted environments.[1]

DTLS support for authentication, integrity, confidentiality, non-repudiation and protection against replay attacks. As a transport layer protocol, Applications can provide additional level of security using TLS or SSL.[7] In addition to this, encryption algorithms and end to end authentication can be used to handle different levels of security according to the required.

Conclusion

A glance of current deployment of devices over network in IoT implies the interconnection of devices over internet and thus provides a ground for new applications' development as well as deployment. Considering the security risks that may cause a failure, different protocols are provided by standardized organizations.

In this paper we study briefly about IoT and its security challenges and also provide a survey regarding different IoT protocols. These protocols are standardized and developed by Institute of Electrical and Electronics Engineers (IEEE) and the Internet Engineering Task Force (IETF). Since there are large numbers of developed protocols, only a brief discussion of few protocols is surveyed. The aim of this paper is to provide an overview of standardized protocols along with their security features and the services provided by each protocol.

References

1. Palattella M, Accettura N, Vilajosana X et al. Standardized Protocol Stack for the Internet of (Important) Things, Communications Surveys & Tutorials. 2013; 15(3): 1389-1406. Doi: 10.1109/SURV.2012.111412.00158.
2. Yao X. A Lightweight Multicast Authentication Mechanism for Small Scale IoT Applications", *IEEE Sensors Journal* 2013; 13(10): 3693-3701.
3. Keoh SL, Kumar SS, Tschofenig H. Securing the Internet of Things: A Standardization Perspective. *IEEE Internet of Things Journal* 2014; 1(3): 265-275.
4. Lize G, Jingpei W, Bin S. Trust Management Mechanism for Internet of Things. China Communcication. 2014; 148-156.
5. Hennebert C,Santos JD. Security Protocols and Privacy Issues into 6LoWPAN Stack: A Synthesis. IEEE Internet of Things Journal 1(5): 384-398.
6. He D, Zeadally S. An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment using Elliptic Curve Cryptography. *IEEE Internet of Things Journal* 2013. DOI 10.1109/JIOT.2014.2360121.
7. Cirani S.IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios. *IEEE Sensors Journal* 2015; 15(2): 1224-1234.
8. Ren K. Guest Editorial Special Issue on Security for IoT: The State of the Art *IEEE Internet of Things Journal* 2014; 1(5): 369-370.
9. Granjal J, Monteiro E, Silva JS. Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues. IEEE Communications Surveys & Tutorials. 2015. DOI 10.1109/COMST.2015.2388550.
10. Hern JL, Ramos A, Antonio JJ et al. Towards a Lightweight Authentication and Authorization Framework for Smart Objects. *IEEE Journal on Selected Areas in Communications* 2015. DOI 10.1109/JSAC.2015.2393436.

Date of Submission: 2018-10-21

Date of Acceptance: 2018-11-20